C087 Certification Report
MarkLogic Server 9

File name: ISCB-3-RPT-C087-CR-v1
Version: v1
Date of document: 22 December 2017
Document classification: PUBLIC

For general inquiry about us or our services,
please email: mycc@cybersecurity.my

CyberSecurity Malaysia
(726630-U)
Best Brand Internet Security 2008 & 2009
MS ISO/IEC 17021: 2011 ISMS 02082013 CB 02
Status Company
T +603 8992 6888
F +603 8992 6841
H 1 300 88 2999

Corporate Office:
Level 5, Sapura@Mines
No 7, Jalan Tasik
The Mines Resort City
43300 Seri Kembangan
Selangor Darul Ehsan
Malaysia.

www.cybersecurity.my

C087 Certification Report
MarkLogic Server 9

22 December 2017
ISCB Department

CyberSecurity Malaysia
Level 5, Sapura@Mines,
No 7 Jalan Tasik,The Mines Resort City
43300 Seri Kembangan, Selangor, Malaysia
Tel: +603 8992 6888 Fax: +603 8992 6841
http://www.cybersecurity.my

Document Authorisation

DOCUMENT TITLE:	C087 Certification Report
DOCUMENT REFERENCE:	ISCB-3-RPT-C087-CR-v1
ISSUE:	v1
DATE:	22 December 2017

DISTRIBUTION:	UNCONTROLLED COPY - FOR UNLIMITED USE AND DISTRIBUTION

Copyright Statement

Registered office:

Level 5, Sapura@Mines

No 7, Jalan Tasik,

The Mines Resort City,

43300 Seri Kembangan

Selangor Malaysia

Registered in Malaysia – Company Limited by Guarantee

Company No. 726630-U

Printed in Malaysia

Foreword

The Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme has been established under the 9th Malaysian Plan to increase Malaysia's competitiveness in quality assurance of information security based on the Common Criteria (CC) standard and to build consumers' confidence towards Malaysian information security products.

The MyCC Scheme is operated by CyberSecurity Malaysia and provides a model for licensed Malaysian Security Evaluation Facilities (MySEFs) to conduct security evaluations of ICT products, systems and protection profiles against internationally recognised standards. The results of these evaluations are certified by the Malaysian Common Criteria Certification Body (MyCB) Unit, a unit established within Information Security Certification Body (ISCB) Department, CyberSecurity Malaysia.

By awarding a Common Criteria certificate, the MyCB asserts that the product complies with the security requirements specified in the associated Security Target. A Security Target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the Security Target, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product satisfies the security requirements.

This certification report is associated with the certificate of product evaluation dated 22 December 2017, and the Security Target (Ref [6]). The certification report, Certificate of product evaluation and security target are posted on the MyCC Scheme Certified Product Register (MyCPR) at www.cybersecurity.my/mycc and the Common Criteria Portal (the official website of the Common Criteria Recognition Arrangement).

Disclaimer

The Information Technology (IT) product identified in this certification report and its associate certificate has been evaluated at an accredited and licensed evaluation facility established under the Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme (Ref [4]) using the Common Methodology for IT Security Evaluation, version 3.1 revision 4 (Ref [3]), for conformance to the Common Criteria for IT Security Evaluation, version 3.1 revision 4 (Ref [2]). This certification report and its associated certificate apply only to the specific version and release of the product in its evaluated configuration. The evaluation has been conducted in accordance with the provisions of the MyCC Scheme and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certification report and its associated certificate is not an endorsement of the IT product by CyberSecurity Malaysia or by any other organisation that recognises or gives effect to this certification report and its associated certificate, and no warranty of the IT product by CyberSecurity Malaysia or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Document Change Log

RELEASE	DATE	PAGES AFFECTED	REMARKS/CHANGE REFERENCE
d1	6 December 2017	All	Initial draft
v1	18 December 2017	All	Finalized

Executive Summary

The Target of Evaluation (TOE) is MarkLogic Server 9 from MarkLogic Corporation.
The TOE is an enterprise-class database that provides a set of services used to build content and search applications which query, manipulate and render Extensible MarkUp Language (XML), JSON, text and binary content. Additionally, the TOE provides "Encryption at Rest" functionality to cryptographically protect the data on media.

The scope of evaluation covers the following various major security functions:

- Security Audit
- Cryptographic Support
- User Data Protection
- Identification & Authentication
- Security Management
- Protection of the TSF
- TOE Access

The scope of the evaluation is defined by the Security Target (Ref [6]), which identifies assumptions made during the evaluation, the intended environment for the TOE, the security functional requirements, and the evaluation assurance level at which the product is intended to satisfy the security requirements. Prospective consumers are advised to verify that their operating environment is consistent with the evaluated configuration, and to give due consideration to the comments, observations and recommendations in this certification report.

This report confirms the findings of the security evaluation of the TOE to the Common Criteria (CC) Evaluation Assurance Level 2 (EAL2) Augmented (ALC_FLR.3). This report confirms that the evaluation was conducted in accordance with the relevant criteria and the requirements of the Malaysia Common Criteria Evaluation and Certification (MyCC) Scheme (Ref [4]).

The evaluation was performed by BAE Systems Applied Intelligence MySEF (Malaysia Security Evaluation Facility) and completed on 5 December 2017.

The Malaysia Common Criteria Certification Body (MyCB), as the MyCC Scheme Certification Body, declares that the TOE evaluation meets all the Arrangements on the Recognition of Common Criteria certificates and the product will be listed in the MyCC Scheme Certified Products Register (MyCPR) at www.cybersecurity.my/mycc and the Common Criteria portal (the official website of the Common Criteria Recognition Arrangement) at www.commoncriteriaportal.org.

It is the responsibility of the user to ensure that MarkLogic Server 9 meets their requirements. It is recommended that a potential user of MarkLogic Server 9 refer to the Security Target (Ref [6]), and this Certification Report prior to deciding whether to purchase the product.

Table of Contents

Index of Tables

Index of Figures

1 Target of Evaluation

1.1 TOE Description

1 The TOE is MarkLogic Server 9 from MarkLogic Corporation. The TOE is an enterprise-class database that provides a set of services used to build content and search applications which query, manipulate and render Extensible MarkUp Language (XML), JSON, text and binary content.

2 The TOE is built with a blend of search engine and database architecture approaches specifically designed to index and retrieve XML and JSON content. The TOE's native data formats are XML and JSON, and the data is accepted in an 'as is' form. Content in other formats can be converted to an XML representation or stored as is (in binary or text formats) when loaded into the TOE. As an XML/JSON database, the TOE manages its own content repository and is accessed using the W3C standard XQuery language, just as a relational database is a specialized server that manages its own repository and is accessed through Structured Query Language (SQL).

3 The TOE is fully transactional, runs in a distributed environment and can scale to terabytes of indexed content. It is schema independent and all loaded documents can be immediately queried without normalizing the data in advance. It provides developers with the functionality and programmability, using XQuery as its query language, to build content-centric applications. Developers build applications using XQuery both to search the content and as a programming language in which to develop applications. It is possible to create entire applications using only MarkLogic Server, and programmed entirely in XQuery. Applications can also be created using Java, JavaScript or other programming languages that access MarkLogic Server.

4 The functionality defined in the Security Target (Ref [6]) that was subsequently evaluated is as follows:

- Security Audit
- Cryptographic Support
- User Data Protection
- Identification & Authentication
- Security Management
- Protection of the TSF
- TOE Access

1.2 TOE Identification

5 The details of the TOE are identified in Table 1 below.

Table 1: TOE identification

Evaluation Scheme	Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme
Project Identifier	C087
TOE Name	MarkLogic Server 9 (ML9)

TOE Version	9
Security Target Title	MarkLogic Essential Enterprise 9 Security Target
Security Target Version	1.0
Security Target Date	8 November 2017
Assurance Level	Evaluation Assurance Level 2 (EAL2) Augmented (ALC_FLR.3)
Criteria	Common Criteria for Information Technology Security Evaluation, September 2012, Version 3.1, Revision 4 (Ref [2])
Methodology	Common Criteria for Information Technology Security Evaluation, September 2012, Version 3.1, Revision 4 (Ref [3])
Protection Profile Conformance	None
Common Criteria Conformance	CC Part 2 Extended CC Part 3 Conformant Package conformant to EAL 2 with Augmented ALC_FLR.3
Sponsor	Leidos Inc 6841 Benjamin Franklin Drive, Columbia MD, 21046, USA
Developer	MarkLogic Corporation 999 Skyway Road, Suite 200, San Carlos CA, 94070, USA
Evaluation Facility	BAE Systems Applied Intelligence – MySEF Level 28 Menara Binjai, 2 Jalan Binjai, 50450, Wilayah Persekutuan Kuala Lumpur, Malaysia

1.3 Security Policy

6 There are no organisational security policies that have been defined regarding the use of TOE.

1.4 TOE Architecture

7 The TOE includes both logical and physical boundaries which are described in Section 2.2 of the Security Target (Ref [6]).

8 The TOE consists of two subsystems, the Administration subsystem and the Server subsystem. The Administration subsystem provides the Admin Interface to the Server subsystem. The Admin Interface application manages all features of the Server subsystem. It is composed of XQuery programs which are evaluated inside of an HTTP server. The HTTP server evaluates each request and sends a response back as a web page to the requester. The Admin Interface is accessed through HTTPS only (i.e., HTTP over TLS).

9 The TOE supports three interfaces that are available through a network. An HTTP server offers connectivity for the administrative interface and for customer applications with the Server subsystem. The communication pathways to and from the Server subsystem are depicted in Figure 1 by the lines labelled as "TLS". Two additional programmatic interfaces are provided by XDBC and ODBC protocols that can also use TLS to protect the session. Developers write client applications to use these interfaces in a system that requires access to a backend XML database. In particular, the HTTP and XDBC servers each provide the Admin API, Security API, and PKI API, which are collections of XQuery functions. The API functions are evaluated inside the HTTP and XDBC servers. Consequently, the servers enforce TOE security policy (for example, authentication, security management restrictions, access control, and auditing). The ODBC server provides read-only access to SQL views that are defined in the context database for that App Server, and is authenticated and authorized based on DAC policy.

10 The TOE includes REST APIs, a Java Client API, and XCC libraries. These libraries are for application development. They do not provide any security functionality. The REST APIs are implemented as XQuery programs that run on an HTTP server. The Java Client API is implemented in Java, and calls the REST APIs, which in turn run on an HTTP server. The HTTP server is an interface to the TOE that honors DAC policy. The XCC libraries run against an XDBC server, which is also an interface to the TOE that honors DAC policy.

11 The following Figure 1 shows the components that comprise the evaluated configuration of the TOE.

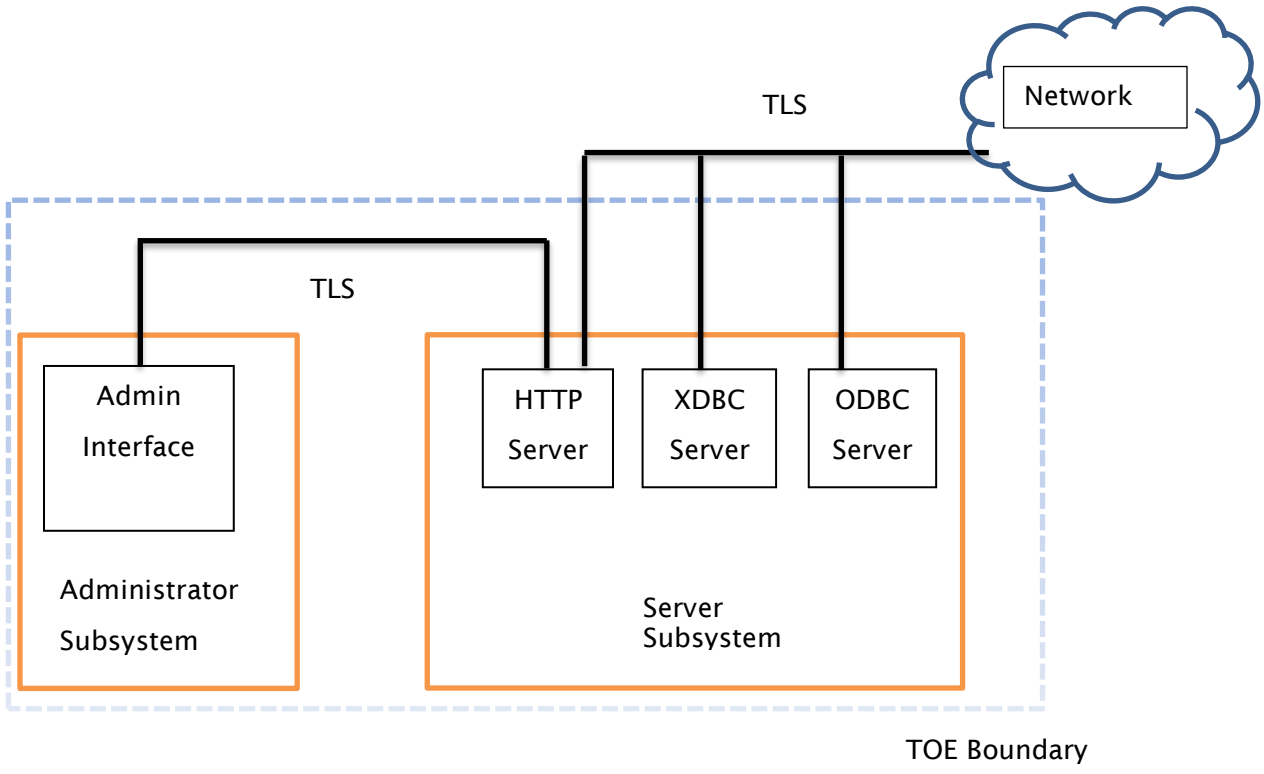

Figure 1: TOE Architecture

1.4.1 Logical Boundaries

12 The scope of the evaluation was limited to those claims made in the Security Target (Ref [6]) and includes only the following evaluated security functionality in Table 2:

Table 2: Logical Boundaries

Security function	Description
Security Audit	The TOE generates audit records that include date and time of the event, subject identity and outcome for security events. The TOE provides authorized administrators with the ability to include and exclude auditable events based on user identity, role, event type, object identity and success and failure of auditable security events. When appropriate, the TOE also associates audit events with the identity of the user that caused the event. The TOE relies on the operational environment for secure storage of the audit records and for system clock information that is used by the TOE to timestamp each audit record.
Cryptographic Support	The Transport Layer Security (TLS) protocol is used to provide protection of the communications surrounding the remote administrative sessions from disclosure and from undetected modification. The TOE supports TLS v1.0, v1.1, and v1.2. For communication between a customer application on a network and the HTTP server, XDBC server, or ODBC server of the TOE, the TOE offers the use of a TLS session to protect these communications. Finally, the TOE uses a TLS protected channel to distribute TSF data when it is transmitted between distributed parts of the TOE (that is, hosts within a cluster); and to transmit MarkLogic-generated keys to trusted external IT entities. The Advanced Encryption Standard (AES) with 256-bit keys is used for Encryption at Rest data encryption (databases, logs, and config files). The TOE uses OpenSSL object module version 2.0 which has undergone a FIPS 140-2 certification (certificate #1747). The TOE includes an OpenSSL object module built without modification from the source code of the OpenSSL FIPS certification. All references to “the TOE” performing cryptographic operations in this security target are indicating that the TOE is performing the operation through its use of the OpenSSL object module.
User Data Protection	The TOE enforces a Discretionary Access Control (DAC) policy which restricts access to TOE-controlled object(s). Users of the TOE are identified and authenticated by the TOE before any access to the system is granted. Once access to the system is granted, authorization provides the mechanism to control what functions a user is allowed to

Security function	Description
	perform based on the user's role. Access to all TOE-controlled objects is denied unless access, based on role, is explicitly allowed. The authorized administrator role shall be able to access any object regardless of the object's permissions. The TOE also provides amplifications or "amps" which temporarily grant roles to a user only for the execution of a specific function. Therefore, the DAC policy can also be extended by a user who is temporarily granted the privileged role in order to perform a specific "amped" function. The TOE also ensures that any previous information content of a resource is made unavailable upon the allocation of the resource to an object. Memory or disk space is only allocated when the size of the new data is first known, so that all previous data is overwritten by the new data.
Identification & Authentication	The TOE requires users to provide unique identification and authentication data before any access to the system is granted and further restricts access to TOE-controlled objects based on role membership. The TOE maintains the following security attributes belonging to individual users: identity, role membership, and password. The TOE uses these attributes to determine access. The TOE provides a password plug-in functionality that allows administrators to write custom code to require passwords to conform to specific rules (e.g., the number of characters, special characters, and last change date).
Security Management	The security functions of the TOE are managed by authorized administrators via the web-based Admin Interface, or application written using the Admin API, Security API, PKI API, and built-in admin functions. The ST defines the security role of 'authorized administrator'. Authorized administrators perform all security functions of the TOE including managing audit events, Data at Rest, user accounts, access control and TOE sessions.
Protection of the TSF	The TOE provides protection mechanisms for its security functions. One of the protection mechanisms is that users must authenticate and have the appropriate permissions before any administrative operations or access to TOE data and resources can be performed on the system. The TOE also maintains a security domain that protects it from interference and tampering by untrusted subjects within the TOE scope of control. Communication with remote administrators is protected by TLS, which protects against the disclosure and undetected modification of data

Security function	Description
	exchanged between the TOE and the administrator. Communication with remote customer applications can also utilize TLS to protect against the disclosure and undetected modification of data exchanged between the TOE and the customer application. Customer applications must determine whether the use of TLS is necessary for that specific customer application's data. TLS protects all MarkLogic-generated keys transmitted from the TSF to trusted external third-party KMS from unauthorised disclosure during transmission. The TOE ensures that TSF data is encrypted and remains consistent when transmitted between parts of the TOE. The TOE provides consistency of TSF data between distributed parts of the TOE by regularly monitoring the configuration file and security database for changes and distributing the updated configuration file or security database to all parts of the cluster. The TOE utilizes a TLS protected channel to distribute TSF data among a cluster.
TOE Access	The TOE restricts the maximum number of concurrent sessions that belong to the same user by enforcing an administrator configurable number of sessions per user. The TOE also denies session establishment based on attributes that can be set explicitly by authorized administrators including role identity, time of day and day of week. Upon successful session establishment, the TOE stores and retrieves the date and time of the last successful session establishment to the user. It also stores and retrieves the date and time of the last unsuccessful session establishment and the number of unsuccessful attempts since the last successful session establishment. This information is collected by the TOE Access security function, because the information pertains to user's attempts to access the TOE. The information gathered by the TOE pertains to historical session establishment actions by a user.

1.4.2 Physical Boundaries

13 The TOE consists of the software applications and network protocol interfaces (described and shown in Figure 1: TOE Architecture above). The Administration subsystem, which provides the Admin Interface, runs using a supported browser, Firefox, Internet Explorer, or Chrome. The Server subsystem applications and network interfaces execute on Linux operating system. The TOE requires the following hardware and OS platforms in its operational environment:

Memory, Disk Space, and Swap Space Requirements

The host system must meet the following minimum requirements:

- 512 MB of system memory, minimum. 2 GB or more recommended, depending on database size.
- 1.5 times the disk space of the total forest size. More specifically, each forest on a filesystem requires its filesystem to have at least 1.5 times the forest size in disk space (or, for each forest less than 32GB, 3 times the forest size).
- Swap space equal to the amount of physical memory on the machine.

Supported Platforms – Server Subsystem

The evaluated configuration of the TOE is supported on Red Hat Enterprise Linux 7 (x64). Note, the deadline I/O scheduler is required on Red Hat Linux platforms. The deadline scheduler is optimized to ensure efficient disk I/O for multi-threaded processes, and the TOE can have many simultaneous threads. In addition, the redhat-lsb, glibc (both the 32-bit and the 64-bit packages) and gdb packages are required.

Supported Platforms – Administration Subsystem

The Administration subsystem is supported on the following browsers in the evaluated configuration:

- Firefox on Windows and Mac OS
- Internet Explorer on Windows
- Chrome on Windows and Mac OS.

Other browser/platform combinations may work but are not as thoroughly tested by MarkLogic.

14 The TOE can be deployed on a single machine or in a distributed environment across multiple machines. In a distributed environment, the TOE is a cluster of hosts. The hosts communicate using TLS to protect transmitted data from disclosure or undetected modification.

15 The TOE relies on the hosting OS to protect its applications, processes, and any locally stored data. The TOE itself maintains a security domain that protects it from interference and tampering by untrusted subjects within the TOE scope of control. Web browsers in the environment are used to access the Admin Interface and the HTTP server through its HTTPS interface, and to terminate a session. The Admin Interface prompts the user to authenticate with a valid username and password in order to log in for a session. As is standard in browser-based applications, the browser caches and automatically re-issues the login credentials for each request throughout the browser session. These credentials are valid until the browser is closed, which terminates the session. When the browser is restarted, the user will once again be prompted to authenticate with a valid username and password.

16 A customer application on the network can also communicate with the TOE's App Servers (HTTP, XDBC or ODBC). The TOE supports the use of TLS versions 1.0, 1.1 and 1.2. The TOE requires applications that use the Admin API, Security API, and PKI API to communicate with the HTTP App Server and XDBC App Server using TLS. Customer client applications are not part of the TOE.

17 An optional external third party KMS is permitted in the evaluated configuration and is assumed to be a trusted external IT. The functionality of external third party KMS is not covered in the scope of the evaluation.

18 The TOE can be configured to use external authentication entities (Kerberos or LDAP) to authenticate users. The TOE can also be configured to authenticate the MarkLogic

Server specifically as a client to external authentication systems: Kerberos, LDAP and AWS. Kerberos, LDAP and AWS are provided by the operational environment.

1.5 Clarification of Scope

19 Section 1.4 of this document described the scope of the evaluation which was limited to those claimed made in the Security Target (Ref [6]).

20 Potential consumers of the TOE are advised that some functions and services of the overall product have not have been evaluated as part of this evaluation. Potential consumers of the TOE should carefully consider their requirements for using functions and services outside of the evaluated configuration.

1.6 Assumptions

21 The assumptions regarding the operational environment and the intended usage of the TOE have been defined in the Security Target (Ref [6]). Consumers should understand their own IT environments and the security aspects of the environment/configuration in which the product is intended to operate.

1.7 Evaluated Configuration

22 The TOE consists of two subsystems, the Administration subsystem and the Server subsystem within the TOE boundary. The Administration subsystem provides the Admin Interface to the Server subsystem and is accessed via supported browsers (Firefox, Internet Explorer or Chrome) over HTTPS only. The Server subsystem handles the work of processing requests from the HTTP, ODBC, and XDBC Server interfaces.

23 The TOE can be deployed on a single machine or in a distributed environment across multiple machines. In a distributed environment, the TOE is a cluster of hosts as covered in the evaluated configuration. The evaluated configuration of the TOE is supported on Red Hat Enterprise Linux 7 (x64) and configuration requires that all communications between the TOE and its components occur over TLS, which provides confidentiality and integrity of transmitted data.

24 The TOE supports the following external entities in the operational environment and in its evaluated configuration:

- Kerberos, LDAP and AWS to support user authentication

25 The TOE also supports an external third party KMS however it was not covered in the scope of the evaluation.

1.8 Delivery Procedures

26 The evaluators examined the delivery documentation and determined that it describes all procedures that are necessary to maintain security when distributing versions of the TOE or parts of it to the consumer.

27 The delivery procedures should consider, if applicable, issues such as:

- ensuring that the TOE received by the consumer corresponds precisely to the evaluated version of the TOE;

- avoiding or detecting any tampering with the actual version of the TOE;
- preventing submission of a false version of the TOE;
- avoiding unwanted knowledge of distribution of the TOE to the consumer: there might be cases where potential attackers should not know when and how it is delivered;
- avoiding or detecting the TOE being intercepted during delivery; and
- avoiding the TOE being delayed or stopped during distribution.

28 The delivery process for the TOE is described in the Delivery Procedures document of the Life Cycle evidences.

1.9 Documentation

29 It is important that the TOE is used in accordance with guidance documentation in order to ensure secure usage of the product.

30 The following documentation is provided by the developer to the end user as guidance to ensure secure delivery, installation and operation of the product.

a) MarkLogic Server Administrator's Guide, May 2017, Last Revised: 9.0-3, September 2017

b) MarkLogic Security Guide, May 2017, Last Revised: 9.0-3, September 2017

c) MarkLogic Server Installation Guide for All Platforms, May 2017, Last Revised: 9.0-3, September 2017

d) MarkLogic Common Criteria Evaluated Configuration Guide, May 2017, Last Revised: 9.0-1, May 2017

2 Evaluation

31 The evaluation was conducted in accordance with the requirements of the Common Criteria, version 3.1 Revision 4 (Ref [2]) and the Common Methodology for IT Security Evaluation (CEM), version 3.1 Revision 4 (Ref [3]). The evaluation was conducted at Evaluation Assurance Level 2 (EAL2) Augmented (ALC_FLR.3). The evaluation was performed conformant to the MyCC Scheme Policy (MyCC_P1) (Ref [4]) and MyCC Scheme Evaluation Facility Manual (MyCC_P3) (Ref [5]).

2.1 Evaluation Analysis Activities

32 The evaluation activities involved a structured evaluation of the TOE, including the following components:

- The evaluators' testing consisted of independent testing efforts, which comprise both functional and penetration test cases to address testing requirements for ATE_IND.2 and AVA_VAN.2 evaluation components.
- For functional testing, the focus was on testing the claimed security functionality (SFRs within the ST) through the interfaces specified in the functional specification (TSFI). For the penetration testing, the effort was limited to attacks that are commensurate to an attacker with equal or less than Basic attack potential. The testing approach for both testing commensurate with the respective assurance components (ATE_IND.2 and AVA_VAN.2).

2.1.1 Life-cycle support

2.1.1.1 Configuration Management Capability

33 The evaluators confirmed that the TOE provided for evaluation is labelled with its reference.

34 The evaluators confirmed that the TOE references used are consistent.

35 The evaluators examined the method of identifying configuration items to determine that it describes how configuration items are uniquely identified.

36 The evaluators examined the configuration items to determine that they are identified in a way that is consistent with the CM documentation.

2.1.1.2 Configuration Management Scope

37 The evaluators confirmed that the configuration list includes the following set of items:

a) the TOE itself;

b) the parts that comprise the TOE; and

c) the evaluation evidence required by the SARs in the ST.

38 The evaluators confirmed that the configuration list uniquely identifies each configuration item.

39 The evaluators confirmed that the configuration list indicates the developer of each TSF relevant configuration item.

2.1.1.3 TOE Delivery

40 The evaluators examined the delivery documentation and determined that it describes all procedures that are necessary to maintain security when distributing versions of the TOE or parts of it to the consumer.

2.1.1.4 Systematic Flaw Remediation

41 The evaluator examined the flaw remediation procedures documentation and determined that it describes the procedures used to track all reported security flaws in each release of the TOE.

42 The evaluator examined the flaw remediation procedures and determined that the application of these procedures would produce a description of each security flaw in terms of its nature and effects, as well as the status of finding a correction to that flaw.

43 The evaluator checked the flaw remediation procedures and determined that the application of these procedures would identify the corrective action for each security flaw.

44 The evaluator examined the flaw remediation procedures documentation and determined that it describes a means of providing the TOE users with the necessary information on each security flaw.

45 The evaluator examined the flaw remediation procedures and determined that the application of these procedures would result in a means for the developer to receive from TOE user reports of suspected security flaws or requests for corrections to such flaws.

46 The evaluator examined the flaw remediation procedures and determined that the application of these procedures would result in a timely means and automatic distribution of providing the registered TOE users who might be affected with reports about, and associated corrections to, each security flaw.

47 The evaluator examined the flaw remediation procedures and determined that the application of these procedures would help to ensure that every reported flaw is corrected and that TOE users are issued remediation procedures for each security flaw.

48 The evaluator examined the flaw remediation procedures and determined that the application of these procedures would result in safeguards that the potential correction contains no adverse effects.

49 The evaluator examined the flaw remediation guidance and determined that the application of these procedures would result in a means for the TOE user to provide reports of suspected security flaws or requests for corrections to such flaws.

50 The evaluator examined the flaw remediation guidance and determined that it describes a means of enabling the TOE users to register with the developer.

51 The evaluator examined the flaw remediation guidance and determined that it identifies specific points of contact for user reports and enquiries about security issues involving the TOE.

2.1.2 Development

2.1.2.1 Architecture

52 The evaluators examined the security architecture description and determined that the information provided in the evidence is presented at a level of detail commensurate with the descriptions of the SFR-enforcing abstractions contained in the functional specification and TOE design.

53 The security architecture description describes the security domains maintained by the TSF.

54 The initialisation process described in the security architecture description preserves security.

55 The evaluators examined the security architecture description and concluded that it contains sufficient information to demonstrate that the TSF is able to protect itself from tampering by untrusted active entities. The security architecture description presents an analysis that adequately describes how the SFR-enforcing mechanisms cannot be bypassed.

2.1.2.2 Functional Specification

56 The evaluators examined the functional specification and determined that:

- the TSF is fully represented,
- it states the purpose of each TSF Interface (TSFI),
- the method of use for each TSFI is given.

57 The evaluators also examined the presentation of the TSFI and determined that:

- it completely identifies all parameters associated with every TSFI; and
- it completely and accurately describes all error messages resulting from an invocation of each SFR-enforcing TSFI.

58 The evaluators also confirmed that the developer supplied tracing that links the SFRs to the corresponding TSFIs.

2.1.2.3 TOE Design Specification

59 The evaluators examined the TOE design and determined that the structure of the entire TOE is described in terms of subsystems. The evaluators also determined that all subsystems of the TSF are identified. The evaluators determined that interactions between the subsystems of the TSF were described.

60 The evaluators examined the TOE and determined that each SFR supporting or SFR-non-interfering subsystem of the TSF was described such that the evaluators could determine that the subsystem is not SFR-enforcing.

61 The evaluators found the TOE design to be a complete, accurate, and detailed description of the SFR-enforcing behaviour of the SFR-enforcing subsystems.

62 The evaluators examined the TOE design and determined that it provides a description of the interactions among SFR-enforcing subsystems of the TSF, and between the SFR-enforcing subsystems of the TSF and other subsystems of the TSF.

63 The evaluators determined that the TOE design contained a complete and accurate mapping from the TSFI described in the functional specification to the subsystems of the TSF described in the TOE design.

64 The evaluators determined that all SFRs were covered by the TOE design, and concluded that the TOE design was an accurate instantiation of all SFRs.

2.1.3 Guidance documents

2.1.3.1 Operational Guidance

65 The evaluators examined the operational user guidance and determined that it describes, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings. For each role, the secure use of available TOE interfaces is described. The available security functionality and interfaces are described for each user role – in each case, all security parameters under the control of the user are described with indications of secure values where appropriate.

66 The operational user guidance describes, for each user role, each type of security-relevant event relative to the user functions that need to be performed, including changing the security characteristics of entities under the control of the TSF and operation following failure or operational error.

67 The evaluators examined the operational user guidance in conjunction with other evaluation evidence and determined that the guidance identifies all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

68 The evaluators determined that the operational user guidance describes, for each user role, the security measures to be followed in order to fulfil the security objectives for the operational environment as described in the ST.

69 The evaluators found that the operational user guidance is clear and reasonable.

2.1.3.2 Preparation Guidance

70 The evaluators examined the provided delivery acceptance and determined that they describe the steps necessary for secure acceptance of the TOE in accordance with the developer's delivery procedures.

71 The evaluators determined that the provided installation procedures describe the steps necessary for secure installation of the TOE and the secure preparation of the operational environment in accordance with the security objectives in the ST.

72 The evaluators performed all user procedures necessary to prepare the TOE during testing and determined that the TOE and its operational environment can be prepared securely using only the supplied preparative user guidance.

2.1.4 IT Product Testing

73 Testing at EAL2 consists of assessing developer tests, performing independent functional tests, and conducting penetration tests. The TOE testing was conducted by evaluators of BAE Systems Applied Intelligence MySEF. The detailed testing activities, including configurations, procedures, test cases, expected results and actual results are documented in a separate Test Plan Report.

2.1.4.1 Assessment of Developer Tests

74 The evaluators verified that the developer has met their testing responsibilities by examining their test plans, and reviewing their test results, as documented in the Evaluation Technical Report (Ref [7]) (not a public document because it contains information proprietary to the developer and/or the evaluator).

75 The evaluators analysed the developer's test coverage and found them to be complete and accurate. The correspondence between the tests identified in the developer's test documentation and the interfaces in the functional specification, TOE design and security architecture description was complete.

2.1.4.2 Independent Functional Testing

76 At EAL2, independent functional testing is the evaluation conducted by evaluator based on the information gathered by examining design and guidance documentation, examining developer's test documentation, executing sample of the developer's test plan, and creating test cases that are independent of the developer's tests.

77 All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. The results of the independent functional tests were recorded by the evaluators and are consistent with the expected test results in the test documentation.

Table 3: Independent Functional Test

Identifier	Description	Security Function
TEST-IND-001-ADM	To test and verify that the following security functionality provided by the TOE performs correctly and as expected: • The TOE audit capability generates an audit record for the defined set of auditable events triggered by user actions, and that each event is associated to the identity of a user. • The audit capability allows the selection of events to be audited from the set of all auditable events based on pre-defined attributes. • The identification and authentication controls in place enforces security attributes to be defined for each TOE user, thus requiring users to be successfully identified and authenticated before allowing access to the TSF and TSF data. • Only authorised administrators are allowed to manage the TOE security management configuration. • The TSF data transmitted between	FAU_GEN.1.1, FAU_GEN.1.2, FAU_GEN.2.1, FAU_SEL.1.1, FIA_UAU.2.1, FIA_UID.2.1, FIA_UAU.5.1, FIA_UAU.5.2, FIA_ATD.1.1, FMT_MTD.1.1(1), FMT_MTD.1.1(2), FMT_SMR.1.1, FMT_SMR.1.2, FMT_SMF.1.1, FTP_TRP.1.1, FTP_TRP.1.2, FTP_TRP.1.3, FPT_ITT.1.1, FPT_TRC_EXT.1

Identifier	Description	Security Function
	parts of the TOE is consistent. • The TOE Admin Interface is accessed through HTTP over TLS (HTTPS).	
TEST-IND-002-ADM	To test and verify that the following security functionality provided by the TOE performs correctly and as expected: • Only authorised administrators are allowed to manage TSF data. • The TOE allows the modification of the maximum number of concurrent sessions belonging to the same user. • The TOE audit capability generates an audit record with the date and time of the last successful session establishment of a user. • The TOE generates an audit record of the date and time of the last unsuccessful login attempt. • The TOE denies session establishment based on user identity or role. • Only authorized administrator is allowed to perform revocation functionality on users.	FAU_GEN.1.1, FAU_GEN.1.2, FAU_GEN.2.1, FTA_MCS.1.1, FTA_MCS.1.2, FTA_TAH_EXT.1.1, FTA_TAH_EXT.1.2, FTA_TSE.1.1, FMT_REV.1.1(1), FMT_REV.1.2(1), FMT_SMF.1.1
TEST-IND-003-XDBC	To test and verify that the following security functionality provided by the TOE performs correctly and as expected: • Verify that user data (documents, directories or collections in MarkLogic server) is protected from unauthorised modification. • Verify that each user can only view or manipulate documents for which they have the proper authorisation (via roles). • Verify compartmental security functionality of the documents. • Verify that the TSF does not store any previous residual information.	FAU_GEN.1.1, FAU_GEN.1.2, FDP_ACC.1.1, FDP_ACF.1.1. FDP_ACF.1.2, FDP_ACF.1.3, FDP_ACF.1.4, FDP_RIP.1.1, FMT_MSA.1.1, FMT_MSA.3.1, FMT_MSA.3.2, FPT_ITT.1.1

Identifier	Description	Security Function
TEST-IND-004-XDBC	To test and verify that the following security functionality provided by the TOE performs correctly and as expected: • The TOE provides a secure communication path between itself and the users. • The TSF data transmitted from the TSF to another trusted IT product is protected from unauthorised disclosure during transmission. • The TOE protects its TSF data from disclosure and modification when transmitting between separate parts of the TOE. • The cipher text should vary for every request.	FCS_CKM.1.1, FCS_CKM.4.1(1), FCS_CKM.4.1(2), FCS_COP.1(1), FTP_TRP.1.1, FTP_TRP.1.2, FTP_TRP.1.3

78 All testing performed by evaluators produced the expected results and as such the TOE behaved as expected.

2.1.4.3 Penetration Testing

79 The evaluators performed a vulnerability analysis of the TOE in order to identify potential vulnerabilities in the TOE. This vulnerability analysis considered public domain sources and an analysis of guidance documentation, functional specification, TOE design, and security architecture description.

80 From the vulnerability analysis, the evaluators conducted penetration testing to determine that the TOE is resistant to attacks performed by an attacker possessing a basic attack potential. The following factors have been taken into consideration during penetration tests:

a) Time taken to identify and exploit (elapse time);

b) Specialist technical expertise required (specialised expertise);

c) Knowledge of the TOE design and operation (knowledge of the TOE);

d) Window of opportunity; and

e) IT hardware/software or other requirement for exploitation.

81 The penetration tests focused on:

a) Unnecessary open ports

b) Infrastructure vulnerability scan

c) Web application scan

d) No-SQL injection

e) Cross-site scripting (XSS)

f) Cross-site request forgery (CSRF)

g) Broken authentication

82 The results of the penetration testing demonstrate that the TOE is resistant to an attacker possessing a basic attack potential. However, it is important to ensure that the TOE is used only in its evaluated configuration and in a secure environment as specified in the Security Target (Ref [6]).

2.1.4.4 Testing Results

83 Tests conducted for the TOE produced the expected results and demonstrated that the product behaved as specified in its Security Target (Ref [6]) and its functional specification. In addition, the documentation supplied as evidence for the EAL2 Augmented ALC_FLR.3 Common Criteria evaluation of the TOE was analysed to identify possible vulnerabilities.

3 Result of the Evaluation

84 After due consideration during the oversight of the execution of the evaluation by the certifiers and of the Evaluation Technical Report (Ref [7]), the Malaysian Common Criteria Certification Body certifies the evaluation of MarkLogic Server 9 performed by BAE Systems Applied Intelligence MySEF.

85 BAE Systems Applied Intelligence MySEF found that MarkLogic Server 9 upholds the claims made in the Security Target (Ref [6]) and supporting documentation, and has met the requirements of the Common Criteria (CC) Evaluation Assurance Level 2 (EAL2) Augmented (ALC_FLR.3).

86 Certification is not a guarantee that the TOE is completely free of exploitable vulnerabilities. There will remain a small level of risk that exploitable vulnerabilities remain undiscovered in its claimed security functionality. The risk is reduced as the certified level of assurance increases for the TOE.

3.1 Assurance Level Information

87 EAL2 Augmented (ALC_FLR.3) provides assurance by a full Security Target and analysis of the SFRs in that Security Target Ref [6]), using functional and interface specifications, guidance documentation and a basic description of the design and architecture of the TOE, to understand the security behaviours of the TOE.

88 The analysis is supported by independent testing of the TSF, evidence of developer testing based on the functional specification, selective independent confirmation of the developer test results, and a vulnerability analysis (based upon the functional specification, TOE design, security architecture description and guidance evidence provided) demonstrating resistance to an attacker possessing a basic attack potential.

89 EAL2 Augmented (ALC_FLR.3) also provides assurance through use of a configuration management system, evidence of secure delivery procedures and systematic flaw remediation.

3.2 Recommendation

90 In addition to ensure secure usage of the product, below are additional recommendations for TOE users:

a) Potential purchasers of the TOE should review the intended operational environment and ensure that they are comfortable that the stated security objectives for the operational environment can be suitably addressed.

b) Potential purchasers of the TOE should ensure that the administrators responsible for the TOE comply with using the supported browsers specified in the ST to access the TOE security functions.

c) Potential purchasers of the TOE should ensure that the browsers used to administer the TOE are configured to securely validate the Administration Server's TLS certificate, either by using a CA signed certificate with the CA

certificate installed in the browsers, or by using a self-signed certificate that is securely imported into the browsers.

Annex A References

A.1 References

[1] Arrangement on the recognition of Common Criteria Certificates in the field of Information Technology Security, July, 2014.

[2] The Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012.

[3] The Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012.

[4] MyCC Scheme Policy (MyCC_P1), v1e, CyberSecurity Malaysia, August 2016.

[5] MyCC Scheme Evaluation Facility Manual (MyCC_P3), v1d, August 2016.

[6] MarkLogic Essential Enterprise 9 Security Target, Version 1.0, 8 November 2017.

[7] Evaluation Technical Report MarkLogic Server 9, Version 1.1, 5 December 2017.

A.2 Terminology

A.2.1 Acronyms

Table 4: List of Acronyms

Acronym	Expanded Term
API	Application Programming Interface
CB	Certification Body
CC	Common Criteria (ISO/IEC15408)
CCRA	Common Criteria Recognition Arrangement
CEM	Common Evaluation Methodology (ISO/IEC 18045)
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standard
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure, HTTP over TLS
IEC	International Electrotechnical Commission
ISO	International Organisation for Standardization
ML9	MarkLogic 9
MyCPR	MyCC Scheme Certified Products Register
MySEF	Malaysian Security Evaluation Facility

Acronym	Expanded Term
MySEF	Malaysian Security Evaluation Facility
ODBC	Open Database Connectivity
PP	Protection Profile
ST	Security Target
TOE	Target of Evaluation
XDBC	XML Database Connector

A.2.2 Glossary of Terms

Table 5: Glossary of Terms

Term	Definition and Source
CC International Interpretation	An **interpretation** of the CC or CEM issued by the CCMB that is applicable to all CCRA participants.
Certificate	The official representation from the CB of the certification of a specific version of a product to the Common Criteria.
Certification Body	An organisation responsible for carrying out **certification** and for overseeing the day-today operation of an **Evaluation and Certification Scheme**. Source CCRA
Consumer	The organisation that uses the certified product within their infrastructure.
Developer	The organisation that develops the product submitted for CC evaluation and certification.
Evaluation	The assessment of an IT product, IT system, or any other valid target as defined by the scheme, proposed by an applicant against the standards covered by the scope defined in its application against the certification criteria specified in the rules of the scheme. Source CCRA and MS-ISO/IEC Guide 65
Evaluation and Certification Scheme	The systematic organisation of the functions of **evaluation** and **certification** under the authority of a **certification body** in order to ensure that high standards of competence and impartiality are maintained and that consistency is achieved. Source CCRA.
Interpretation	Expert technical judgement, when required, regarding the meaning or method of application of any technical aspect of the criteria or the methodology. An interpretation may be either a **national interpretation** or a **CC international interpretation**.

Term	Definition and Source
Certifier	The certifier responsible for managing a specific certification task.
Evaluator	The evaluator responsible for managing the technical aspects of a specific evaluation task.
Maintenance Certificate	The update of a Common Criteria certificate to reflect a specific version of a product that has been maintained under the MyCC Scheme.
National Interpretation	An **interpretation** of the CC, CEM or MyCC Scheme rules that is applicable within the MyCC Scheme only.
Security Evaluation Facility	An organisation (or business unit of an organisation) that conducts ICT security evaluation of products and systems using the CC and CEM in accordance with Evaluation and Certification Scheme policy
Sponsor	The organisation that submits a product for evaluation and certification under the MyCC Scheme. The sponsor may also be the developer.

--- END OF DOCUMENT ---